SEALED

United States District Court

NORTHERN DISTRICT OF TEXAS

In the Matter of the Search of
(Name, address or Brief description of person, property or premises to be searched)
Information Associated with Facebook username account Terrance.Sandifer that is stored at the premises owned, maintained, controlled, or operated by Facebook Incorporated, a social network provider headquartered at 1601 Willow Road, Menlo Park, California 94025

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 3:15-MJ-353-BN

I Kyle Pacatte **being duly sworn depose and say:**

I am a(n) Special Agent with the Internal Revenue Service (IRS) and have reason to believe that on the person of or XX on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A).

in the NORTHERN District of TEXAS there is now concealed a certain person or property, namely (describe the person or property to be seized)

(SEE ATTACHMENT B).

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
property that constitutes evidence of the commission of a crime, contraband, the fruits of crime, and is, otherwise, criminally possessed, **concerning a violation of Title** 18 **United States code, Section(s)** 1028, 1341 and 1343. **The facts to support a finding of Probable Cause are as follows:**

(SEE ATTACHED AFFIDAVIT OF SPECIAL AGENT KYLE PACATTE).

Continued on the attached sheet and made a part hereof. XX **Yes** __ **No**

Kyle Pacatte
Signature of Affiant
KYLE PACATTE
Special Agent, IRS

Sworn to before me, and subscribed in my presence

May 26, 2015 **at** **Dallas, Texas**
Date **City and State**

DAVID L. HORAN
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

ATTACHMENT A

Property to be Searched

The premises to be searched is all information associated with the Facebook username Terrance.Sandifer that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California. The information to be searched should include from January 1, 2014 through the present date, all stored data, information, and/or communications and other files reflecting data, information, and/or communications to or from Facebook username Terrance.Sandifer.

The premises to be searched should also include all stored records, data, and information associated with any account associated with or related to the Facebook user name Terrance.Sandifer from January 1, 2014 through the present date.

ATTACHMENT B

Items to be Seized

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under Title 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user or account listed in Attachment A:

a. All contact and personal identifying information, including full name, user, identification number, email address(es), birthdate, gender, Facebook passwords, Facebook security questions and answers, physical address(es) (including city, state, and ZIP code), telephone numbers, screen names, websites, and other personal identifiers.

b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

c. All photos or videos uploaded by the username and the associated location information, and all photos or videos uploaded by any user that have the username tagged in them and the associated location information;

d. All profile information; news feed information; status updates; links to videos, photos, articles, and other items; notes; wall postings; friend

lists, including the friends' Facebook username; groups and networks of which the user is a member, including the groups's Facebook group identification number; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

f. All "check ins" and other location information;

g. All IP logs, including all records of the IP addresses that logged into the account;

h. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "Liked";

i. All information about the Facebook pages that the account is or was a "fan" of;

j. All past and present lists of friends created by the account;

k. All records of Facebook searches performed by the account;

l. All information about the user's access and use of Facebook Marketplace;

m. The types of service utilized by the user;

n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit/debit card or bank account number);

o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

p. All records pertaining to communications between Facebook and any person regarding the user of the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18 U.S.C. § 1028 (Fraud and related activity in connection with identification documents), Title 18 U.S.C. § 1341(Mail Fraud), and Title 18 U.S.C. § 1343 (Wire Fraud), including but not limited to:

a. all records containing, discussing, referring of relating to any income tax returns or preparation of income tax returns;

b. identification documents;

c. cashier's checks or tax refund checks;

d. receipt, transmission, possession of any personal identifying information of others;

e. all communications discussing, relating to or regarding U.S. Treasury checks or cashier's checks;

f. all records relating to who created, used, or communicated with the user, including records about their identities and whereabouts.

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Kyle Pacatte, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook username that is stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the username.

2. I am a Special Agent employed by Internal Revenue Service, Criminal Investigation (IRS-CI) and have served in this capacity since September 2009. A Special Agent's duties include investigations of violations of Internal Revenue laws and related offenses, money laundering statutes, and Bank Secrecy Act requirements. I received training in investigative techniques at the Federal Law Enforcement Training Center in Glynco, Georgia. I also received specialized training in the investigation of violations of the Internal Revenue laws and related financial crimes, and have participated in investigations of these offenses and been the affiant on various warrants. In addition to my experience as a Special Agent, I earned a Bachelor of Business Administration in Accounting concurrently with a

Masters of Business Administration from the University of Texas at Arlington in 2003. I am a Certified Public Accountant licensed in the state of Texas, and a Certified Fraud Examiner.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. 1028 (Fraud and related activity in connection with identification documents), Title 18 U.S.C. § 1341(Mail Fraud), and Title 18 U.S.C. § 1343 (Wire Fraud), have been committed by Terrance Sandifer, Roderick Linson, Jason Rabb, and other unknown co-conspirators. There is also probable cause to search the information described in Attachment A for evidence and fruits of these crimes, as described in Attachment B.

Background of Investigation/Overview of Scheme

5. Each year, taxpayers have the option of either mailing their Federal income tax return to the Internal Revenue Service (IRS) or filing their tax return electronically. If a taxpayer is due a refund, there are several options for payment. A refund check can be mailed to the taxpayer's residence or the refund can be directed to the taxpayer's bank account or pre-paid card by including bank routing

and account information in the appropriate section of the return. Taxpayers and/or return preparers may also purchase financial products from software providers. With the financial product, once the IRS authorizes the refund, the product software captures the refund information and allows the return preparer to receive their return preparation fees from the taxpayer's refund and provide the refund to the taxpayer in the form of a check, direct deposit or pre-paid card. A return preparer typically receives blank check stock from the financial product software provider and once the authorization is received, the return preparer can print a refund check for the taxpayer.

6. Santa Barbara Tax Products Group (TPG) provides tax-related financial products as described above, receiving tax refunds from the IRS and directing payments to preparers and/or software providers and remitting the balance of the refund to the taxpayer as provided in the agreement.

7. On March 4, 2014, Christopher Bagg, Risk Administrator for TPG, contacted IRS-CI about ongoing fraud involving 87 of TPG's tax refund checks totaling $452,236. In the scheme, two refund checks were being negotiated at approximately the same time for each refund. The original, or 'real', refund check was typically negotiated at a bank by the legitimate taxpayer. The second, or 'false', check was cashed at a Walmart store in the Dallas, Texas area by an unknown person.

8. Each 'real' and 'false' check was for the exact same amount, the amount owed to the taxpayer. Both checks included the exact same Magnetic Ink

Character Recognition (MICR) information on the bottom of the check. The refunds involved varying amounts issued to different taxpayers who had tax returns prepared by various tax return preparers, using various tax software programs. There was no bright line or common thread, other than TPG. TPG recognized the scheme first, since both checks were being presented for payment. Since all the false checks were cashed at Walmarts, TPG alerted Walmart to the scheme.

9. On March 28, 2014, Walmart Global Investigator Clint Lee ("Lee") provided surveillance photos of the transactions where the false checks were cashed, including vehicles used by the people conducting the transaction. The Texas license plate of a vehicle, a red Chevrolet Impala (the "Impala"), was discernible. The Impala was seen delivering and picking up the check cashers in numerous transactions, but the driver did not appear to enter the Walmarts with the check cashers.

10. On March 31, 2014, I contacted Avis/Budget rental cars, the owner of the Impala. The car had been rented to Jason Rabb since January 29, 2014, and was still rented to him at the time of the contact.

11. The identities of the people cashing the false checks are unknown. How the subjects are able to obtain the check information, including the exact amount of the refund payable to the taxpayer, the taxpayer's name, social security number, etc. is unknown. How an appropriate false identity document is created

in order to present to the Walmart associate who cashes the false check is also unknown.

Probable Cause

12. On March 16, 2015, I met with Lee about the ongoing scheme. Amongst others cashed in 2015, TPG alerted Walmart the false checks below were cashed at Walmarts in the area:

Check No.	Payee	Amount	Date	Time	Walmart Location	
3585551	Farrah Soto	$4,223.10	02/18/2015	19:42	7401 Samuell Blvd., Dallas, TX	"Samuell Store"
3585562	Ricky Viola	$6,290.66	02/19/2015	15:36	1521 N. Cockrell Hill, Dallas, TX	"Cockrell Hill Store"
3585563	Karry Osornia	$2,534.10	02/19/2015	18:08	200 Short Street, Dallas, TX	"Short Store"
3585573	Harold Jones	$3,585.10	02/19/2015	19:08	150 N. Interstate 35E, Lancaster, TX	"Lancaster Store"
3585569	Charles Rayfield	$3,927.10	02/20/2015	15:00	108 W. Parkerville Road, DeSoto, TX	"DeSoto Store"
	TOTAL	$20,560.06				

13. Lee provided surveillance photos of all 2015 transactions to date on March 17, 2015. According to Lee, two Walmart Asset Protection Associates ("APA") separately identified a person in multiple transactions as Terrance Sandifer ("Sandifer"). One of those APAs recognized a second person as Roderick 'Rocky' Linson ("Linson") in other transactions. Both of the APAs went to Kimball High School as did Sandifer and Linson. An APA works in plain clothes at a Walmart location and attempts to prevent theft or loss of Walmart assets.

14. On March 19, 2015, I interviewed "APA1" at the Walmart location where s/he works in Lancaster, Texas ("Lancaster store"). APA1 positively identified Sandifer as the person who cashed false check number 3585573 in the amount of $3,585.10 payable to "Harold Jones" in a February 19, 2015 transaction

at the Lancaster store. APA1 showed me surveillance video from the Lancaster store that day. APA1 talked to Sandifer after Sandifer received approximately $3,585.10 less Walmart fees after cashing the false check. At the time, APA1 did not suspect any wrongdoing by Sandifer, but did note that Sandifer seemed nervous. APA1 thought Sandifer was cashing his own tax refund because Sandifer was carrying a folder. APA1 walked with Sandifer as he was heading to the exit. APA1 saw Linson waiting for Sandifer in the McDonald's inside Walmart near the exit. APA1 talked to Linson and overheard Sandifer on the phone telling someone that he had run into a "cousin" that worked at Walmart in loss prevention. APA1 understood s/he was the "cousin" Sandifer was referring to. Sandifer and Linson left together. Sandifer knows APA1 works at Walmart as an APA.

15. APA1 and Sandifer are not close but they grew up in the same area in Oak Cliff, went to high school together, and are friends on Facebook. Sandifer's Facebook name is "Terrance T Sand Sandifer". During the interview, APA1 described a Facebook item posted by Sandifer on the same day, February 19, 2015, as the encounter with APA1 at the Lancaster store. The post was a picture of someone's lap, presumably Sandifer's, with several $100 bills spread out as the person was seated in a vehicle and a comment about "Blood Money" . APA1 had seen the post prior to talking to Sandifer as described above. APA1 mentioned the post when s/he talked to Sandifer. APA1 attempted to show me the

post, but was unable to view it on his/her smartphone. APA1 thought perhaps Sandifer had deactivated his Facebook account.

16. Including the transaction above, APA1 recognized Sandifer in the following surveillance photos from Walmarts where false checks were cashed:

Check No.	Payee	Amount	Date	Time	Walmart Location	
3585551	Farrah Soto	$4,223.10	02/18/2015	19:42	7401 Samuell Blvd., Dallas, TX	"Samuell Store"
3585562	Ricky Viola	$6,290.66	02/19/2015	15:36	1521 N. Cockrell Hill, Dallas, TX	"Cockrell Hill Store"
3585573	Harold Jones	$3,585.10	02/19/2015	19:08	150 N. Interstate 35E, Lancaster, TX	"Lancaster Store"

APA1 pointed out distinctive pants Sandifer was wearing in the Cockrell Hill store photo. APA1 noticed the pants in the Facebook photo with the $100 bills described above, and APA1 recalls them from the interaction with Sandifer at the Lancaster store later that same day.

17. APA1 reviewed surveillance photos from other Walmarts where false checked were cashed and thought the person in the photos looked like Linson:

Check No.	Payee	Amount	Date	Time	Walmart Location	
3585563	Karry Osornia	$2,534.10	02/19/2015	18:08	200 Short Street, Dallas, TX	"Short Store"
3585569	Charles Rayfield	$3,927.10	02/20/2015	15:00	108 W. Parkerville Road, DeSoto, TX	"DeSoto Store"

18. On March 20, 2015, I interviewed "APA2" at the Walmart location where s/he works, the Samuell store. APA2 positively identified Sandifer from surveillance photos related to false checks at the Lancaster, Cockrell Hill, and Samuell stores. APA2 did not recognize Linson from his Texas Driver's License picture; s/he does not know him.

19. APA2 saw and talked to Sandifer at the Samuell store in late January or early February. Sandifer was buying something; he was not cashing a check. APA2 does not know if Sandifer knows that APA2 works at Walmart as an APA.

20. APA2 and Sandifer are not close but they grew up in the same area in Oak Cliff, went to high school together, and are friends on Facebook. APA2 accessed Sandifer's Facebook page, under "Terrance T Sand Sandifer" on his/her smartphone during the interview. APA2 showed me a Sandifer post from February 19, 2015 at 4:49pm. The post appears to be the post described by APA1 with the several $100 bills. APA2 also noted that Sandifer appeared to be wearing the same clothes and shoes in a February 18, 2015 post at 11:13am as in the surveillance photos from the Samuell store on the same day. APA2 provided me screenshots of the Facebook posts.

21. Based on my knowledge and experience with Facebook, since APA2 was able to access Sandifer's Facebook page, but APA1 was not able to, I believe APA1 was "defriended" by Sandifer sometime after the encounter at the Lancaster store.

22. On March 24, 2015, TPG provided check copies and data about the 'real' and 'false' checks. Each of the real checks was related to a tax return filed for the payee. The false checks have the same check number, included the same last name, address, the last four digits of the Social Security Number ("SSN"), and were for the same amount. However, the first names are different on the false checks:

CHECK No.	AMOUNT	Last Name	FALSE First Name	Real First Initial
3585569	$3,927.10	RAYFIELD	CHARLES	G
3585551	$4,223.10	SOTO	FARRAH	J
3585562	$6,290.66	VIOLA	RICKY	T
3585573	$3,585.10	JONES	HAROLD	D
3585563	$2,534.10	OSORNIA	KARRY	R

23. False check number 3585551 cashed at Walmart by Sandifer according to APA1 and APA2 is payable to "Farrah Soto". Handwritten on the check is "TX XXXX2590 DOB XX/XX/83 Ex XX/XX/21"[1]. Based on my training and experience, XXXX2590 is the Texas Driver's License number, XX/XX/83 is the date of birth ("DOB"), and XX/XX/21 is the expiration of the Driver's License provided to the teller by the check casher. On April 7, 2015, I researched the Texas Department of Public Safety Driver License Image Retrieval System. Driver's License XXXX2590 comes back to J Soto[2], with the correct DOB, address, and expiration date.

24. False check number 3585562 cashed at Walmart is payable to "Ricky Viola". Handwritten on the check is "TX XXXX6023 DOB XX-XX-82 EXP XX/XX/21". Based on my training and experience, XXXX6023 is the Texas Driver's License number, XX/XX/82 is the DOB, and XX/XX/21 is the expiration of the Driver's License provided to the teller by the check casher. On April 7, 2015, I researched the Texas Department of Public Safety Driver License Image Retrieval System. Driver's License XXXX6023 comes back to T Viola, a white female, with the correct DOB and expiration date.

[1] The Texas Driver's License numbers and dates of birth are redacted to protect the privacy of the real taxpayers.
[2] Only first Initials are used for the real taxpayers to protect their privacy.

25. False check number 3585563 cashed at Walmart is payable to "Karry Osornia". Handwritten on the check is "DL TX XXXX1387 DOB XX/XX/84 EX XX/XX/21". Based on my training and experience, XXXX1387 is the Texas Driver's License number, XX/XX/84 is the DOB, and XX/XX/21 is the expiration of the Driver's License provided to the teller by the check casher. On April 7, 2015, I researched the Texas Department of Public Safety Driver License Image Retrieval System. Driver's License XXXX1387 comes back to R Osornia, with the correct DOB, address, and expiration date.

26. False check number 3585569 cashed at Walmart is payable to "Charles Rayfield". Handwritten on the check is "XXXX7949 XX-XX-1984". Based on my training and experience, XXXX7949 is the Texas Driver's License number, and XX/XX/84 is the DOB on the Driver's License provided to the teller by the check casher. On April 7, 2015, I researched the Texas Department of Public Safety Driver License Image Retrieval System. Driver's License XXXX7949 comes back to G Rayfield, with the correct DOB.

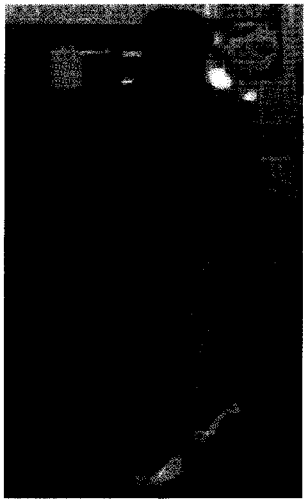
27. False check number 3585573 cashed at Walmart is payable to "Harold Jones". Handwritten on the check is "DOB 1/25/84 – 3/10/15". Based on my training and experience, 01/25/84 is the DOB as provided to the teller by the check casher. On April 7, 2015, I researched the Texas Department of Public Safety Driver License Image Retrieval System. Driver's License XXXX8424 for D Jones, a black female, shows her DOB is 01/25/84.

28. Based on the surveillance photos provided by Walmart, the Facebook posts provided by APA2, and the information provided by TPG, Sandifer and Linson cashed the false checks using fraudulent identity documents. The Walmart personnel are not suspected of being a part of the scheme.

29. Surveillance photos provided by Lee identified by APA1 and APA2 as Terrance Sandifer:

Walmart Picture 1
2/18/2015
Approximately 17:42
Samuell Store
"Farrah Soto" Jones"

Walmart Picture 2
02/19/2015
Approximately 15:36
Cockrell Hill Store
"Ricky Viola"



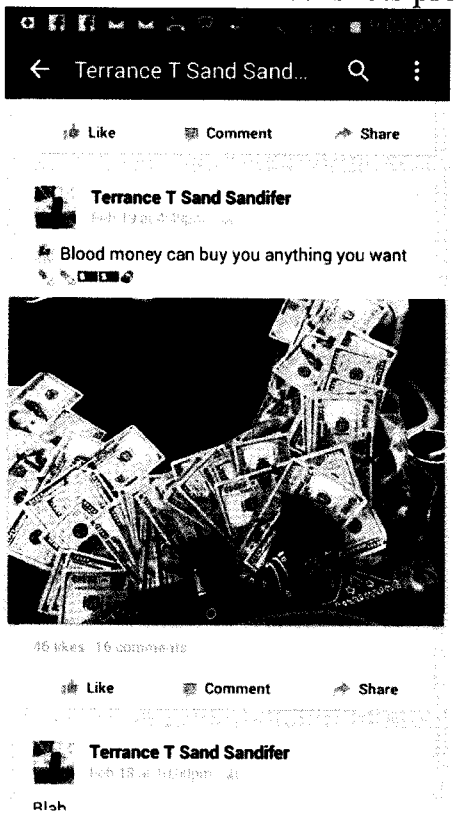
Walmart Picture 3
02/19/2015
Approximately 19:08
Lancaster Store
"Harold

30. Surveillance photos provided by Lee looks like Roderick "Rocky" Linson according to APA1:

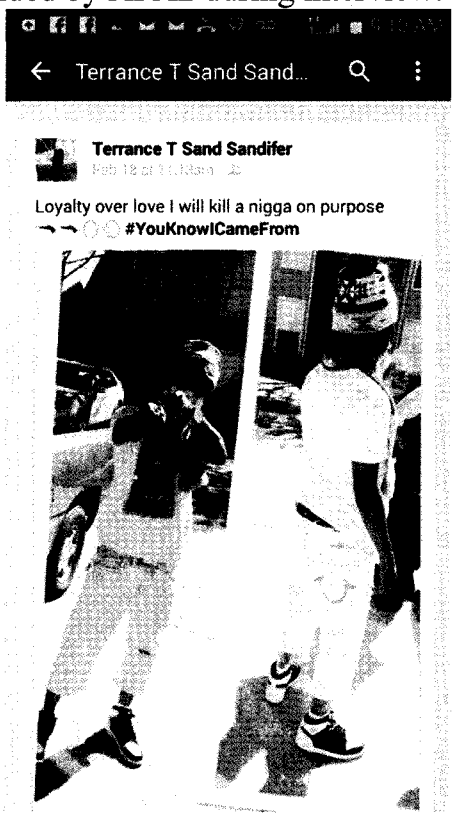
Walmart Picture 4
2/19/2015
Approximately 18:08
Short Street Store
"Karry Osornia"

Walmart Picture 2
02/20/2015
Approximately 15:00
DeSoto Store
"Charles Rayfield"

31. Facebook screenshots provided by APA2 during interview:



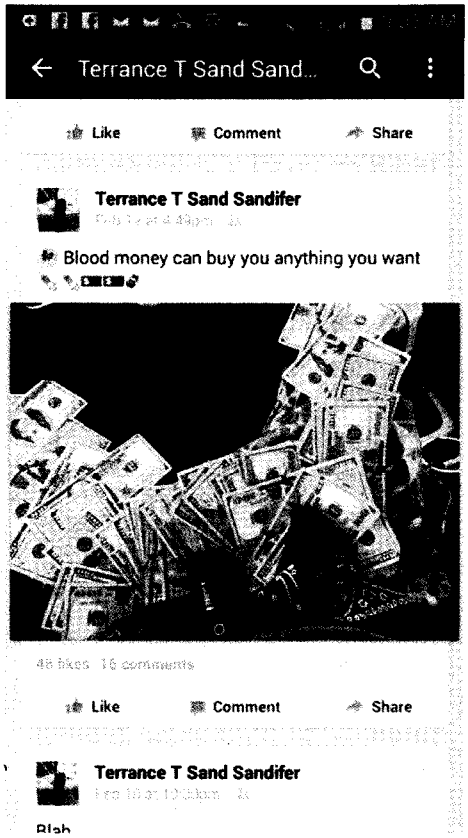
Facebook 1
2/19/2015
4:49pm



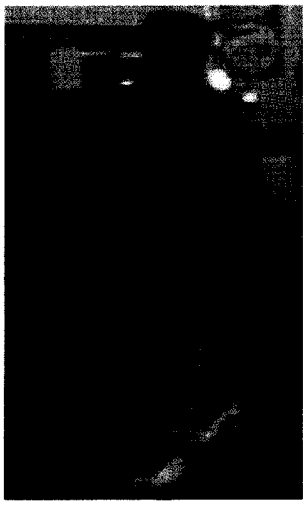
Facebook 2
2/18/2015
11:13am

32. Comparison: Walmart and Facebook photos, same pants on Sandifer according to APA1:

Walmart Picture 2
02/19/2015
Approximately 15:36
Cockrell Hill Store



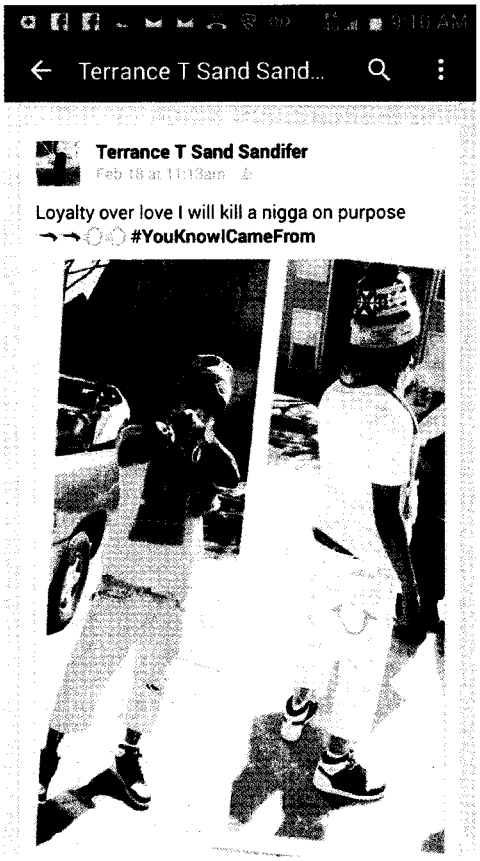
Facebook 1
02/19/2015
4:49pm (16:49)



Walmart Picture 3
02/19/2015
Approximately 19:08
Lancaster Store

33. Comparison: Walmart to Facebook photos, same pants and shoes according to APA2

Walmart Picture 1
2/18/2015
Approximately 17:42
Samuell Store



Facebook 2
2/18/2015
11:13am

Facebook

34. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

35. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or

thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

36. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

37. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users

can adjust to control, for example, the types of notifications they receive from Facebook.

38. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

39. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

40. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

41. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

42. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

43. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

44. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the

present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

45. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

46. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

47. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

48. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

49. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the

administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook also assigns a group identification number to each group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and/or administrator, as well as a PDF of the current status of the group profile page.

50. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

51. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log

would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

52. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

53. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

54. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of

communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

55. Based on the forgoing, I request that the Court issue the proposed search warrant.

56. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

57. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

58. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation.

59. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Kyle Pacatte
Special Agent
IRS-CI

Subscribed and sworn to before me on May 26, 2015

DAVID L. HORAN
UNITED STATES MAGISTRATE JUDGE